DNS Pentesting

Sunny Neo
Santosh Ananthakrishnan

Why DNS?

- DNS is not typically considered an attack vector
- Firewalls allow outbound requests to port 53!
- Google’s Ron Bowes: Pentesting with DNS

Background

- Previous attacks on DNS typically exploit the protocol directly - Kaminsky etc.

- Using DNS as the vector for other web attacks instead, is fun and hard to detect because DNS is ‘trusted’

Why it Matters

- New exploit vectors possible that won’t get detected
- Filtering high volume DNS is expensive. Major CDNs are very abusive of the infrastructure
- Getting data stolen Considered Harmful

Fun with TXT Records

- Sites like http://who.is were until recently vulnerable to script injection in the TXT records
- Searching for the whois record of a domain with a malicious TXT record caused arbitrary javascript execution.

DNS Recon

XSS Testing:

- Add <img src= “xsstest.mydomain.com”>
- Watch DNS server logs for a request

Blind SQLi

- Conditionally force a DNS request. If we receive it, the condition must be true

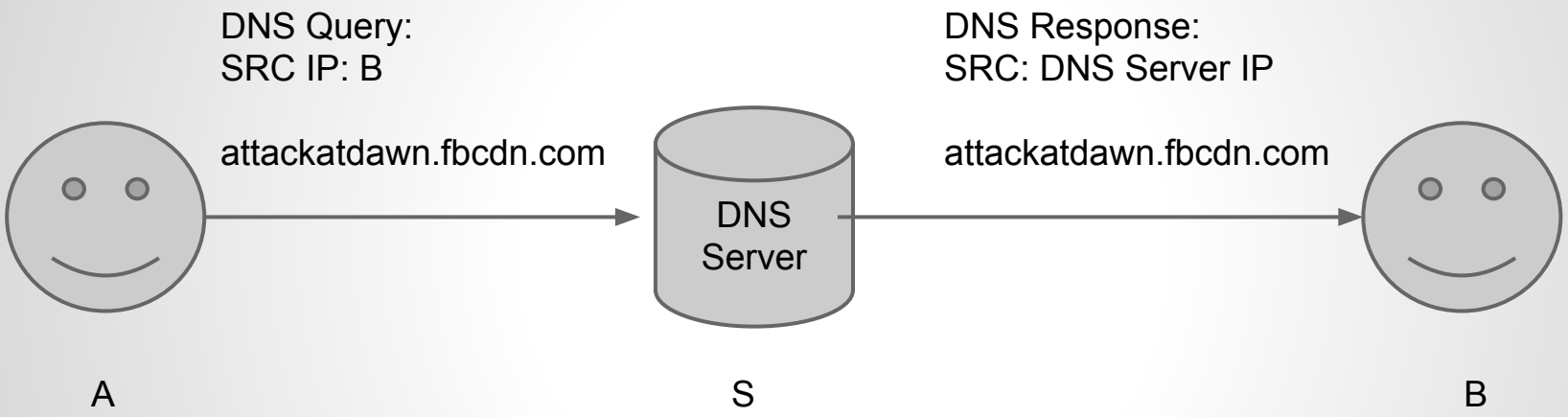
Tunneling over DNS

- Utilize hostname for upstream data and the queries in the Answer or Additional Records for downstream data
- SSH can be tunneled across DNS - dnscat2 fits any byte stream onto DNS
- Effectively bypass all IDS/Firewall/Proxy - who filters port 53 anyway?

Proposal

- Implement DNS-based attacks as a Metasploit module
- Add more functionality, besides the attacks discussed in the BSides talk [1]
- One idea : DNS Reflection - Covert, communication through any arbitrary non-participating third party.

DNS Reflection



Proposed Timeline

- Oct 24 : Finalize functionality target for Version 1
- Nov 1 : Complete feasibility test for DNS Reflection
- Nov 21 : Implement all proposed functionality
- Dec 1 : Test, document extensively and release module

Proposed Evaluation

- DNS Reflection Evaluation
  - Data throughput and reliability
  - Security and privacy concerns

- Functionality test and release module
  - The novelty here is that such a toolkit does not exist

References

[1] https://tc.gtisc.gatech.edu/bss/2014/r/dns-hacking.pdf

[2] https://wiki.skullsecurity.org/Dnscat